UNIWERSYTET KARDYNAŁA STEFANA WYSZYŃSKIEGO W WARSZAWIE

Załącznik nr 3 do SWZ

OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest zakup licencji na oprogramowanie antywirusowe wraz z funkcją szyfrowania całych dysków – 2 000 sztuk na okres 36 miesięcy.
2. Zamawiający posiada licencje ESET antywirus i ESET Full Disk Encryption:
2.1. Liczba chronionych stacji roboczych, urządzeń mobilnych i serwerów: 2 000 sztuk.
2.2. Licencja ważna do: 11 czerwca 2024 roku
2.3. Identyfikator publiczny licencji: 33B-UJW-D9N
2.4. Identyfikator publiczny licencji: 3AN-DVV-PAD
3. Licencje na system zabezpieczający przed złośliwym oprogramowaniem, zostaną dostarczone w terminie 5 dni roboczych od daty zawarcia umowy. Dostarczone licencje mogą zostać aktywowane w dniu 12 czerwca 2024 roku.
4. Przedmiot zamówienia obejmuje dostawę licencji na system zabezpieczający przed złośliwym oprogramowaniem i zapewniającym szyfrowanie dysków, zwane dalej „Systemem", na okres 36 miesięcy od dnia 12 czerwca 2024 roku dla 2000 sztuk stacji roboczych, urządzeń mobilnych i serwerów plików.
5. Wykonawca dostarczy dokumenty licencyjne m.in. certyfikat, warunki licencjonowania oraz klucz licencyjny i instrukcje instalacji do Oprogramowania na adres e-mail (e-mail: licencje@uksw.edu.pl).
6. Udzielona na System licencja musi umożliwiać co najmniej:
6.1. dostęp do subskrypcji aktualnych baz sygnatur;
6.2. dostęp do najnowszej wersji oprogramowania;
6.3. wsparcia technicznego producenta lub dystrybutora oprogramowania;
7. Parametry i funkcjonalności dostarczonego Systemu, nie mogą być gorsze niż wskazane poniżej:
7.1. System musi zapewniać ochronę antywirusową:
7.1.1. serwera plików,
7.1.2. stacji roboczych,
7.1.3. urządzeń przenośnych (smartfony, tablety),
7.2. Dla stacji roboczych system musi ponadto zapewnić kontrolę podłączanych urządzeń (np. pamięci USB, zewnętrzne napędy, itp.).
7.3. Konfiguracja, nadzór nad pracą poszczególnych modułów oraz instalacja na stacjach roboczych winna być wykonywana z centralnej konsoli zarządzającej dostarczonej w ramach przedmiotu zamówienia przez Wykonawcę.
7.4. Wsparcie techniczne powinno odbywać się w języku polskim przez cały czas trwania umowy (jako serwis telefoniczny bądź za pomocą poczty elektronicznej).
7.5. Moduł ochrony antywirusowej, antispyware i ransomware musi poprawnie współpracować z następującymi systemami operacyjnymi wykorzystywanymi przez Zamawiającego: Microsoft Windows, Linux i macOS.

7.6. Moduł ochrony stacji roboczych musi posiadać polskojęzyczny interfejs i zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.
7.7. Moduł ochrony antywirusowej musi:
7.7.1. Realizować ochronę na podstawie:
7.7.1.1. sygnatur,
7.7.1.2. heurystyki (z możliwością jej wyłączenia),
7.7.1.3. na bieżąco weryfikowanej informacji o nowych zagrożeniach w bazie producenta dostępnej przez Internet;
7.7.2. posiadać możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony;
7.7.3. umożliwiać skanowanie antywirusowe w chwili dostępu (real time), na żądanie i według harmonogramu z następującymi warunkami:
7.7.3.1. skanowanie na żądanie i według harmonogramu mieć możliwość przerwania w dowolnym momencie,
7.7.3.2. skanowanie na żądanie z możliwością wstrzymania w przypadku wykrycia pracy na baterii lub w przypadku wykrycia pracy w trybie pełnoekranowym (np. prezentacja);
7.7.4. wykrywać zagrożenia: na dyskach, w plikach w tym archiwach plikowych, na stronach web, w przesyłkach email w tym w załącznikach, na podłączanych nośnikach przenośnych;
7.7.5. zapewniać ochronę komunikacji przy wykorzystaniu protokołów POP3, SMTP i IMAP w czasie rzeczywistym niezależnie od klienta pocztowego;
7.7.6. zapewniać ochronę komunikacji przy wykorzystaniu protokołu HTTP w czasie rzeczywistym niezależnie od przeglądarki;
7.7.7. zawierać programy (plugin-y do przeglądarek Microsoft IE, Mozilla Firefox i Google Chrome) działające na stacjach użytkowników i ostrzegające ich o złośliwej zawartości strony internetowej wraz z możliwością aktywnego blokowania dostępu do wybranych stron internetowych, określonych centralnie przez administratora systemu. Rozwiązanie musi realizować także możliwość określenia blokowanych stron web na podstawie kategorii strony (np. pornografia, strony społecznościowe, itp.) lub moduł musi umożliwiać blokowanie stron na podstawie predefiniowanych kategorii oraz konkretnych adresów URL, w określonych przez administratora przedziałach czasu;
7.7.8. umożliwiać ustawienia priorytetu procesu skanowania;
7.7.9. realizować aktualizację wzorców wirusów musi odbywać się co najmniej raz dziennie;
7.7.10. umożliwiać aktualizację wzorców wirusów z archiwum internetowego lub z centralnego punktu dystrybucji wzorców wirusów;
7.7.11. mieć możliwość pobierania aktualizacji za pośrednictwem serwera Proxy;

7.7.12. po wykryciu zagrożenia posiadać możliwość oczyszczenia zainfekowanego pliku, a jeśli nie jest to możliwe – usunięcia bądź umieszczenia go w lokalnej kwarantannie;
7.7.13. w przypadku zainstalowania na urządzeniach przenośnych nastąpić automatyczna zmiana punktu dystrybucji wzorców na archiwum internetowe bez konieczności ingerencji użytkownika;
7.7.14. umożliwiać konfigurowanie dostępności i zakresu ingerencji użytkownika w proces skanowania;
7.7.15. pozwolić na zabezpieczanie hasłem przed zmianą konfiguracji, deinstalacją i zatrzymaniem programu;
7.7.16. wymuszać odświeżanie wzorców wirusów;
7.7.17. uaktualniać silnik oprogramowania i bazy wzorców wirusów przez cały okres trwania abonamentu (trwania umowy).
8. Moduł szyfrowania całych dysków.
8.1. System musi zapewniać pełną zgodność z RODO z możliwością drukowania niezbędnych raportów
8.2. Zarządzanie procesem szyfrowania/deszyfrowania powinno być możliwe z tej samej konsoli co system antywirusowy.
8.3. System szyfrowania danych winien wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 7/8/8.1/10/11 32-bit i 64-bit.
8.4. System szyfrowania winien wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
8.5. Aplikacja powinna koniecznie posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć również możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
8.6. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
9. Moduł ochrony urządzeń mobilnych.
9.1. Ochronę urządzeń pracujących pod kontrolą wykorzystywanych przez Zamawiającego systemów Android oraz Apple iOS.
9.2. Ochronę plików w czasie rzeczywistym.
9.3. Skanowanie plików systemowych, bibliotek, plików archiwum oraz innych.
9.4. Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
9.5. Ochronę proaktywną wykrywającą nieznane zagrożenia.
9.6. Określenie poziomu głębokości skanowania plików archiwum.
9.7. Określenie domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
9.8. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.
9.9. Włączenie blokady urządzenia mobilnego na hasło alfanumeryczne o zadanej złożoności: np. minimum 8 znaków składających się z liter małych i dużych, oraz cyfr i znaków specjalnych.

9.10. Ustalenie czasu, po którym włącza się blokada urządzenia (np. blokada ekranu po 5 minutach nieaktywności użytkownika).
9.11. Pamięć historii haseł blokady urządzenia, wykluczająca możliwość użycia co najmniej 5 ostatnich haseł.
9.12. Możliwość wykrywania ingerencji w oryginalne oprogramowanie urządzenia.
9.13. Możliwość blokowania aplikacji po jej nazwie.
9.14. Możliwość zarządzania dedykowaną konsolą on-line.
10. Moduł centralnej konsoli zarządzającej musi:
10.1. zapewnić centralną instalację programów służących do ochrony stacji roboczych Windows oraz urządzeń mobilnych na OS Android;
10.2. zapewnić centralne zarządzanie wszystkimi programami służącymi do ochrony: stacji roboczych, serwerów plików, serwerów pocztowych, serwerów portalu wielofunkcyjnego, aplikacji mobilnych;
10.3. posiadać centralną bazę przechowującą informacje o konfiguracji stacji i urządzeń końcowych;
10.4. posiadać centralną bazę przechowującą informacje o zdarzeniach i wykrytych zagrożeniach;
10.5. umożliwić zdalną instalację produktów na komputerach z domeny Microsoft Active Directory objętych ochroną, bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania z wyprzedzeniem momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów;
10.6. oferować rozwiązania umożliwiające selektywne wskazanie, który z produktów ochronnych wchodzących w skład systemu zostanie wdrożony na którym z komputerów – nie jest dopuszczalne wdrożenie pakietu w postaci jednej paczki instalacyjnej obejmującej kilka produktów na raz;
10.7. posiadać możliwość definiowania komputerów, które mają być objęte wdrożeniem poszczególnych produktów, musi być możliwe na bazie zdefiniowanych grup maszyn oraz na bazie dynamicznie przydzielanych znaczników, niezależnie od podziału na grupy maszyn, uzależnionych od parametrów komputera - co najmniej takich jak: rodzaj CPU, ilość RAM, wielkość dysku, rodzaj systemu operacyjnego, ilość dostępnego miejsca na dysku;
10.8. niekoniecznie zawierać dodatkowego agenta do centralnej instalacji i zarządzania na instancji serwera;
10.9. szyfrować komunikację między serwerem a klientami;
10.10. zapewnić centralną konfigurację i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci;
10.11. być wyposażony w kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł w oparciu o reguły odczytane ze wszystkich lub z wybranych komputerów lub ich grup;

10.12. posiadać możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej;
10.13. mieć możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych);
10.14. mieć możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy;
10.15. umożliwiać centralną aktualizację stacji roboczych z serwera w sieci lokalnej lub z Internetu;
10.16. mieć możliwość utworzenia centralnego punktu dystrybucji wzorców wirusów;
10.17. mieć możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych;
10.18. posiadać możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów;
10.19. posiadać możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci;
10.20. mieć możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne);
10.21. posiadać możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na wykorzystywanych przez Zamawiającego stacjach z systemem Windows;
10.22. koniecznie posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP i syslog lub wywołania komendy/skryptu;
10.23. winna mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory;
10.24. koniecznie umożliwiać zdefiniowanie wielu kont administratorów i przydzielenie im szczegółowych ról umożliwiających co najmniej: ograniczenie dostępu do wskazanych grup maszyn, ograniczenie administracji do poszczególnych produktów i ich specyficznych funkcji.

11. Opis równoważności.
11.1. Zamawiający dopuszcza możliwość dostawy rozwiązania równoważnego realizującego funkcje i spełniającego wymagania opisane w pkt. 8-11 oraz zapewniające dodatkowo:
11.1.1. Dostawę oprogramowania i urządzeń o wydajności i funkcjonalności nie gorszej od posiadanych przez Zamawiającego.
11.1.2. Zapewnienie usługi kompletnej nieinwazyjnej deinstalacji dotychczasowego oprogramowania antywirusowego i systemu antyspamowego z całej infrastruktury informatycznej (komputerów, serwerów i urządzeń mobilnych) Zamawiającego.
11.1.3. Zapewnienie usługi kompletnej nieinwazyjnej instalacji i konfiguracji nowego rozwiązania w infrastrukturze informatycznej Zamawiającego.
11.1.4. Zapewnienia dodatkowego wsparcia technicznego (zdalnego oraz w razie potrzeby, bezpośredniego – realizowanego w siedzibie Zamawiającego) przez Wykonawcę przez okres miesiąca od daty wdrożenia produkcyjnego rozwiązania równoważnego.
11.1.5. Przeszkolenie do 5 pracowników Zamawiającego z zakresu obsługi, konfiguracji i administracji całości rozwiązania równoważnego.
11.1.6. Wdrożenie, szkolenie, asysta techniczna i dodatkowe wsparcie techniczne Wykonawcy – w języku polskim w siedzibie Zamawiającego.
11.1.7. Usługi wdrożeniowe równoważnego oprogramowania antywirusowego i systemu antyspamowego zostaną zrealizowane nie później niż w terminie wygaśnięcia posiadanych przez Zamawiającego licencji.
11.2. Oprogramowanie nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy o Krajowym systemie bezpieczeństwa (Dz.U. 2023 poz 913) dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, Oprogramowanie musi być zgodne z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.
11.3. Warunki licencjonowania mają umożliwiać Zamawiającemu (Licencjobiorcy) objęcie dostarczonym Oprogramowaniem stacji roboczych należących do podmiotów administracji publicznej, na warunkach zdefiniowanych w Opisie Przedmiotu Zamówienia.

11.4. Dostarczana licencja Oprogramowania musi pochodzić z autoryzowanego przez producenta kanału dystrybucji. Wykonawca jest zobowiązany dostarczyć Zamawiającemu dowody poświadczające autentyczność zakupionych licencji na zasadach określonych przez producenta wraz z dostawą Oprogramowania.